



**PATENT APPLICATION**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of

Masanori SATAKE et al.

Application No.: 10/653,217

Filed: September 3, 2003

Docket No.: 116969

For: JOB PROCESSING DEVICE AND DATA MANAGEMENT METHOD FOR THE  
DEVICE

**CLAIM FOR PRIORITY**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested for the above-identified patent application and the priority provided in 35 U.S.C. §119 is hereby claimed:

Japanese Patent Application No. 2003-081445 filed on March 24, 2003

In support of this claim, a certified copy of said original foreign application:

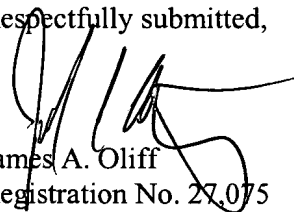
  X   is filed herewith.

           was filed on        in Parent Application No.        filed       .

           will be filed at a later date.

It is requested that the file of this application be marked to indicate that the requirements of 35 U.S.C. §119 have been fulfilled and that the Patent and Trademark Office kindly acknowledge receipt of this document.

Respectfully submitted,

  
James A. Oliff  
Registration No. 27,075

Joel S. Armstrong  
Registration No. 36,430

JAO:JSA/mlo

Date: October 2, 2003

OLIFF & BERRIDGE, PLC  
P.O. Box 19928  
Alexandria, Virginia 22320  
Telephone: (703) 836-6400

DEPOSIT ACCOUNT USE AUTHORIZATION Please grant any extension necessary for entry; Ch...
---

日本国特許庁  
JAPAN PATENT OFFICE

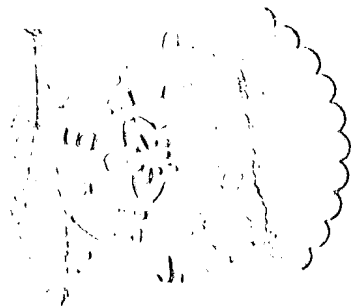
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2003年 3月24日  
Date of Application:

出願番号 特願2003-081445  
Application Number:  
[ST. 10/C]: [JP 2003-081445]

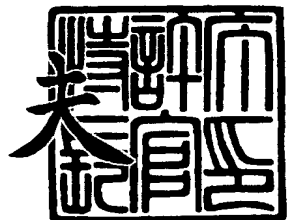
出願人 富士ゼロックス株式会社  
Applicant(s):



2003年 9月10日

特許庁長官  
Commissioner,  
Japan Patent Office

今井 康



出証番号 出証特2003-3074220

【書類名】 特許願

【整理番号】 FE03-00109

【提出日】 平成15年 3月24日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 12/00

【発明者】

    【住所又は居所】 神奈川県海老名市本郷 2 2 7 4 番地 富士ゼロックス株  
式会社海老名事業所内

    【氏名】 佐竹 雅紀

【発明者】

    【住所又は居所】 神奈川県海老名市本郷 2 2 7 4 番地 富士ゼロックス株  
式会社海老名事業所内

    【氏名】 益井 隆徳

【発明者】

    【住所又は居所】 神奈川県海老名市本郷 2 2 7 4 番地 富士ゼロックス株  
式会社海老名事業所内

    【氏名】 横濱 竜彦

【特許出願人】

    【識別番号】 000005496

    【氏名又は名称】 富士ゼロックス株式会社

【代理人】

    【識別番号】 100075258

    【弁理士】

    【氏名又は名称】 吉田 研二

    【電話番号】 0422-21-2340

## 【選任した代理人】

【識別番号】 100096976

【弁理士】

【氏名又は名称】 石田 純

【電話番号】 0422-21-2340

## 【手数料の表示】

【予納台帳番号】 001753

【納付金額】 21,000円

## 【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ジョブ処理装置及び該装置におけるデータ管理方法

【特許請求の範囲】

【請求項 1】 第 1 の記憶装置と、

前記第 1 の記憶装置よりも記憶したデータを高速に消去可能な第 2 の記憶装置と、

前記第 1 の記憶装置と前記第 2 の記憶装置とに、ジョブの実行に供されるジョブデータを振り分けて格納する格納制御部と、

前記格納制御部により前記第 2 の記憶装置に振り分けて格納されたジョブデータを、所定の消去条件が満足された場合に消去する消去部と、  
を備えるジョブ処理装置。

【請求項 2】 請求項 1 に記載のジョブ処理装置であって、

前記格納制御部により前記第 1 及び第 2 の記憶装置に振り分けて格納されたジョブデータを読み出して統合するジョブデータ統合部と、

前記ジョブデータ統合部により統合されたジョブデータに基づき、ジョブを実行するジョブ処理部とを備え、

前記ジョブ処理部によるジョブの実行完了を、前記消去部における所定の消去条件とすることを特徴とするジョブ処理装置。

【請求項 3】 請求項 1 に記載のジョブ処理装置であって、

前記第 2 の記憶装置として揮発性メモリを用いることを特徴とするジョブ処理装置。

【請求項 4】 請求項 1 に記載のジョブ処理装置であって、

前記第 2 の記憶装置として、前記ジョブ処理装置が備える主記憶装置の一部の領域を利用することを特徴とするジョブ処理装置。

【請求項 5】 請求項 1 に記載のジョブ処理装置であって、

前記格納制御部は、前記ジョブデータを暗号化し、その暗号化結果のデータを前記第 1 の記憶装置と第 2 の記憶装置とに振り分けて格納することを特徴とするジョブ処理装置。

【請求項 6】 請求項 1 に記載のジョブ処理装置であって、

前記格納制御部は、所定のルールに従って前記第 1 の記憶装置と前記第 2 の記憶装置とにジョブデータを振り分けて格納し、

前記所定のルールを変更するルール管理部を更に備えるジョブ処理装置。

【請求項 7】 請求項 6 に記載のジョブ処理装置であって、

前記ルール管理部は、自装置の状態に応じて前記所定のルールを変更することを特徴とするジョブ処理装置。

【請求項 8】 請求項 6 に記載のジョブ処理装置であって、

前記ルール管理部は、前記ジョブの属性に応じて前記所定のルールを変更することを特徴とするジョブ処理装置。

【請求項 9】 請求項 1 に記載のジョブ処理装置であって、

前記消去部による前記第 2 の記憶装置に振り分けて格納されたジョブデータの消去後に、前記第 1 の記憶装置に振り分けて格納されたジョブデータを消去する残消去部を備えることを特徴とするジョブ処理装置。

【請求項 10】 ジョブの実行に供されるジョブデータを記憶装置に格納する格納制御部と、

前記格納制御部により前記記憶装置に格納されたジョブデータの一部を、所定の消去条件が満足された場合に消去する消去部と、

を備えるジョブ処理装置。

【請求項 11】 請求項 10 に記載のジョブ処理装置であって、

前記記憶装置からジョブデータを読み出し、読み出したジョブデータを用いて前記ジョブを実行するジョブ処理部を備え、

前記ジョブ処理部によるジョブの実行完了を、前記消去部における所定の消去条件とすることを特徴とするジョブ処理装置。

【請求項 12】 請求項 1 又は 10 に記載のジョブ処理装置であって、

前記消去部における前記所定の消去条件は、ユーザからジョブデータの消去指示を受けることであることを特徴とするジョブ処理装置。

【請求項 13】 請求項 1 又は 10 に記載のジョブ処理装置であって、

前記消去部における前記所定の消去条件は、ユーザからジョブ処理の中止指示を受けることであることを特徴とするジョブ処理装置。

【請求項 14】 請求項 1 又は 10 に記載のジョブ処理装置であって、  
ジョブの実行を制御するジョブ制御部であって、前記消去部によるデータ消去  
処理が完了した時点で別のジョブの実行を許可するジョブ制御部、  
を更に備えるジョブ処理装置。

【請求項 15】 ジョブの実行に供されるジョブデータを、第 1 の記憶装置  
と、これよりもデータ消去が高速な第 2 の記憶装置とに振り分けて格納し、  
格納された前記ジョブデータのうち前記第 2 の記憶装置に記憶したデータ部分  
を、所定の消去条件が満足された場合に消去する、  
ことを特徴とするジョブ処理装置のデータ管理方法。

【請求項 16】 コンピュータに、  
ジョブの実行に供されるジョブデータを、第 1 の記憶装置と、これよりもデー  
タ消去が高速な第 2 の記憶装置とに振り分けて格納する手順と、  
格納された前記ジョブデータのうち前記第 2 の記憶装置に記憶したデータ部分  
を、所定の消去条件が満足された場合に消去する手順と、  
を実行させるためのデータ管理プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、コピー機、プリンタ、ファクシミリ、複合機など、ユーザの要求に  
応じて所定のジョブを実行するジョブ処理装置に関し、特にジョブ処理装置に記  
憶されるデータの秘密保持のための技術に関する。

【0002】

【従来の技術】

近年のデジタル複写機や複合機は、ハードディスク等の大容量記憶装置を搭載  
するものが多い。このような大容量記憶装置は、原稿を複数部数コピーする場合  
や両面印刷を行う場合に原稿画像を一時的に保存したり、スキャン要求に応じて  
原稿読取部で読み取った原稿画像をユーザがネットワークを介してダウンロード  
するまで保存したりするなどの用途に用いられる。

【0003】

近年、ネットワーク化やこれに伴う情報犯罪の増加を背景として、企業の情報セキュリティ管理強化の気運が高まっており、I SMS (Information Security Management System) などの認証制度も始まっている。ハードディスク抜き取りなどによる情報漏洩リスクを考えると、企業の総合的な情報セキュリティ管理においては、デジタル複写機や複合機の大容量記憶装置内に残ったデータも見過ごせない問題である。

#### 【 0 0 0 4 】

この問題に対し、特許文献 1 に示される技術では、複写機に機密文書モードを設け、このモードが設定されている時には、画像データの処理が完了した時点でハードディスク上のその画像データを消去することとしている。

#### 【 0 0 0 5 】

また特許文献 2 に示される技術では、ハードディスクに保存した画像データを複写機のアイドル時間に消去することとしている。

#### 【 0 0 0 6 】

また特許文献 3 に示される技術では、割込ジョブの画像データを割込復帰前に消去するか、割り込まれたジョブの終了後に消去するかを、その画像データのデータ量に応じて決めている。またこの技術では、ユーザが複写機を利用しない放置時間が所定時間を超えた時にハードディスク上の画像データを消去したり、ユーザが複写の中止を指示した時にその複写処理に係る画像データをハードディスクから消去したりしている。

#### 【 0 0 0 7 】

なお、ハードディスク上の画像データの消去は、単にファイルシステム上でその画像データファイルを削除するだけでは、ハードディスク上に実体データが残るため不十分である。そこで、従来より、ハードディスク上の実体データまで消去する場合は、その実体データの領域にランダムなデータを複数回上書きすることが行われている。

#### 【 0 0 0 8 】

また、画像データを暗号化してからハードディスクに格納することで、更にセキュリティを高めることも行われている。



**【 0 0 0 9 】****【特許文献 1】**

特開平 9 - 2 2 3 0 6 1 号公報

**【特許文献 2】**

特開平 9 - 2 8 4 5 7 2 号公報

**【特許文献 3】**

特開 2 0 0 3 - 3 7 7 1 9 号公報

**【 0 0 1 0 】****【発明が解決しようとする課題】**

上記特許文献 1 ～ 3 の技術は、いずれも、ハードディスクからの画像データの消去期間中はハードディスクに対する画像データの読み書きができないため、その間は次の印刷処理や画像読取処理を開始することができない。例えばカラーでページ数の多い原稿など、データ量の多い原稿の処理を行った後は、その原稿の画像データを消去するのに長い時間がかかるため、処理待ちが長くなる。特許文献 3 の技術では、消去処理を行うタイミングを割込その他の条件に応じて制御することで消去処理の影響を低減しようとしているが、いったん消去を始めると消去が完了するまで次の処理を開始できない点は改善されていない。また、特許文献 3 の技術では、消去処理を実行するタイミングが来るまでの間、ハードディスク中に実体データが完全な形で残っている場合があるという問題があった。

**【 0 0 1 1 】****【課題を解決するための手段】**

本発明は、第 1 の記憶装置と、前記第 1 の記憶装置よりも記憶したデータを高速に消去可能な第 2 の記憶装置と、前記第 1 の記憶装置と前記第 2 の記憶装置とに、ジョブの実行に供されるジョブデータを振り分けて格納する格納制御部と、前記格納制御部により前記第 2 の記憶装置に振り分けて格納されたジョブデータを、所定の消去条件が満足された場合に消去する消去部と、を備えるジョブ処理装置を提供する。

**【 0 0 1 2 】**

本発明の好適な態様では、前記第 2 の記憶装置として揮発性メモリを用いる。

## 【0013】

また別の好適な態様では、前記第2の記憶装置として、前記ジョブ処理装置が備える主記憶装置の一部の領域を利用する。

## 【0014】

また別の好適な態様では、前記格納制御部は、前記ジョブデータを暗号化し、その暗号化結果のデータを前記第1の記憶装置と第2の記憶装置とに振り分けて格納する。

## 【0015】

また別の好適な態様では、ジョブ処理装置は、所定のルールに従って前記第1の記憶装置と前記第2の記憶装置とにジョブデータを振り分けて格納するとともに、前記ルールを変更するルール管理部を更に備える。

## 【0016】

ルールの変更は、例えば当該ジョブ処理装置の状態に応じて行うことができる。ここで、ジョブ処理装置の「状態」には、例えば第2の記憶装置の空き容量や書き込み・読み出し速度、ジョブ処理装置の処理負荷、待機中のジョブの有無などがある。

## 【0017】

また別の好適な態様では、ジョブ処理装置は、前記ルールを、前記ジョブの属性に応じて変更するルール管理部を更に備える。ここで、ジョブの「属性」には、ジョブに付与された機密度や、ジョブの対象となる文書の種別などがある。

## 【0018】

## 【発明の実施の形態】

以下、本発明の実施の形態（以下実施形態という）について、図面に基づいて説明する。以下では、本発明の方式を、デジタル複合機などの画像形成装置に適用した場合の例を説明する。すなわち以下では、コピー処理やスキャン処理のための原稿読み取りにより生成された画像データのファイルや、リモートホストから要求された印刷指示やそれを展開した画像データのファイル、受信したファクシミリデータなど、画像形成装置が要求される各種のジョブを実行するために受信したり生成したりしたデータのセキュリティ保護のための仕組みを説明する。

## 【 0 0 1 9 】

まず、図 1 を参照して、本実施形態の画像形成装置のハードウェア構成を説明する。図 1 は、本実施形態の制御の説明のために必要な構成要素を図示したものであり、その他の構成要素については図示を省略している。

## 【 0 0 2 0 】

この画像形成装置は、デジタル複写機やデジタル複合機など、原稿を光学的に読み取って得た画像をデジタルデータとして取り扱うタイプの装置である。

## 【 0 0 2 1 】

この装置において R O M （リード・オンリ・メモリ） 1 2 には、この画像形成装置の動作制御のための制御プログラムなどのデジタル情報が格納されている。C P U （中央処理装置） 1 0 がこの R O M 1 2 内の制御プログラムを実行することにより、画像形成装置の各部の制御が実現される。後述するファイルの格納、読み出し、及び消去の各手順を記述したプログラムも、この R O M 1 2 に格納されている。

## 【 0 0 2 2 】

R A M （ランダム・アクセス・メモリ） 1 4 は、この画像形成装置の主記憶装置であり、制御プログラムの実行の際にワークメモリとしても用いられる。R A M 1 4 は、例えば、プリントエンジン 2 4 に供給する 1 ページ分の画像データを蓄えるページバッファとして用いることもできる。

## 【 0 0 2 3 】

H D D （ハードディスク・ドライブ） 1 6 は、各種のデータを保存するための補助記憶装置である。例えば、H D D 1 6 には、画像形成装置が、要求される各種ジョブのために受信したり生成したりしたジョブデータが保存される。このようなジョブデータとしては、例えば、コピーのためにスキャンエンジン 2 2 で読み取った原稿画像データや、リモートホストから依頼された親展プリント処理（ユーザ認証が成功して初めて印刷を行う処理）の印刷指示データやこれを展開して得られる画像データ、スキャン指示に従ってスキャンエンジン 2 2 で読み取った画像データなどがある。このようなジョブデータのファイルは、ジョブの終了

と共にファイルシステムから削除される。ただし、ファイルシステム上で単にファイルを削除しただけではそのファイルの実体データがHDD上に残るとというのが従来からの問題であり、本実施形態ではその問題に対する新たな解決を提供する。

#### 【0024】

操作パネル18は、この画像形成装置のユーザインタフェースのための表示や、ユーザからの各種指示の入力受付などのためのユーザインタフェース手段である。操作パネル18は、典型的には、コピースタートボタンなどの機械的な操作ボタンや液晶タッチパネルを備える。液晶タッチパネルは、CPU10で実行される制御プログラムが生成したGUI（グラフィカルユーザインタフェース）画面を表示し、そのディスプレイに対するユーザのタッチ位置を検出して制御プログラムに渡す。制御プログラムは、そのタッチ位置の情報からユーザの入力内容を解釈する。

#### 【0025】

通信インタフェース20は、ローカルエリアネットワークなどのネットワークとのデータ通信のための制御を行う装置である。リモートホストからのプリント指示等は、この通信インタフェース20を介して画像形成装置内に入力される。

#### 【0026】

スキャンエンジン22は、原稿を光学的に読み取って電子的な画像データを生成するスキャナ機能を提供する装置である。自動原稿送り装置（ADF）（図示省略）にセットされた原稿は、ADFの機能により1枚ずつスキャンエンジンに送られ、光学的に読み取られる。

#### 【0027】

プリントエンジン24は、CPU10の制御により供給される画像データを用紙に画像形成（印刷）するプリンタ機能を提供する装置である。

#### 【0028】

このような画像形成装置において、本実施形態では、保存するジョブデータファイルのセキュリティ向上のための方策として、従来HDD16に格納されていたジョブデータのファイルを、HDD16とRAM14とに振り分けて格納する

構成をとる。すなわち、1つのジョブデータファイルは、HDD16内の格納ファイル40と、RAM14内の格納ファイルの一部分42とに分けて記憶されることになる。この構成によれば、ジョブデータファイルを消去する場合には、RAM14上の格納ファイルの一部分42を消去すればよい。RAM14内のデータの消去は高速に行うことができる。RAM14内のデータ42を消去した場合、HDD16内に残った格納ファイル40だけでは、元のジョブデータファイルを復元できないので、ジョブデータの秘密を守ることができる。特に、ジョブデータファイルを暗号化してからHDD16とRAM14とに分散格納する構成とすれば、HDD16に残った格納ファイル40は、暗号化したジョブデータファイルから一部を欠落させたものなので、復号処理が非常に困難となり、高いセキュリティを実現できる。

#### 【0029】

図2は、この画像形成装置におけるジョブデータファイルの記憶・読み出し・消去のための機構を示す機能ブロック図である。

#### 【0030】

この構成において、ジョブ制御部100は、操作パネル18や通信インタフェース20から入力されるジョブ要求を受け付け、それら要求に対応するジョブ処理の実行を制御する。ジョブの実行としては、画像形成処理や種々の画像処理、文字認識処理、他装置への送信処理等が挙げられる。実行中のジョブに対する割込ジョブの受付や、その割込に伴うジョブの退避や復帰の制御も、このジョブ制御部100により行われる。また、ジョブ制御部100は、実行するジョブが、ジョブデータの一時保存が必要な場合、その保存を格納・消去処理部110に要求する。なお、ジョブデータの一時保存が必要なジョブには、例えば原稿を複数部数コピーするジョブや、親展プリントのジョブ、あるいは読み取った画像を親展ボックスに一時保管するジョブなどがある。複数部数コピーの場合は、その部数分の印刷出力が完了した時点でジョブが完了し、親展プリントの場合は、画像形成装置でのユーザ認証が成功して印刷出力が完了した時点でジョブが完了する。また、親展ボックスへのスキャン画像の保存処理は、リモートホストがその親展ボックス内のデータをダウンロードした時点でジョブが完了する。

## 【0031】

また、ジョブ制御部100は、いったん保存したジョブデータをジョブ実行のために使用する時が来た場合には、格納・消去制御部110に対してそのジョブデータの読み出しを要求する。

## 【0032】

格納・消去制御部110は、ジョブデータファイルの格納及び読み出しの処理を行うモジュールである。ジョブ制御部100からジョブデータファイルの格納要求があった場合は、格納・消去制御部110は、それらを所定の振り分けルール（又は手順）に従ってRAM14とHDD16に分散格納する。またジョブ制御部100からジョブデータファイルの読み出し要求があった場合は、格納・消去制御部110は、RAM14とHDD16に分散格納したデータを読み出し、振り分けルールに基づいて統合することで元のジョブデータファイルを復元し、ジョブ制御部100に提供する。

## 【0033】

暗号処理部112は、格納・消去制御部110によりRAM14やHDD16に格納するデータを所定の暗号アルゴリズムに従って暗号化したり、RAM14やHDD16から読み出したデータを復号したりする。

## 【0034】

乱数発生部114は、格納・消去制御部110によるRAM14及びHDD16への分散格納処理のために乱数を発生させるモジュールである。

## 【0035】

メモリ監視部116は、RAM14の空き容量を監視するモジュールである。監視により求めた空き容量の情報は、格納・消去制御部110が、ジョブデータのRAM14とHDD16への振り分け量を求めるのに利用される。

## 【0036】

次に図3を参照して、格納・消去制御部110によるジョブデータファイルの格納時の処理を説明する。

## 【0037】

ジョブ制御部100からジョブデータファイルの格納要求を受けた場合、格納

・消去制御部110は、まずそのファイルを暗号処理部112に暗号化させる（S10）。

#### 【0038】

次に格納・消去制御部110は、暗号化したジョブデータのうち、RAM14に格納するデータのサイズを計算する（S12）。この計算は、メモリ監視部116で求めたRAM14の空き容量と、乱数発生部114で発生させた乱数とを用いて、格納サイズを計算する。基本的な考え方は、RAM14の空き容量が多いほど格納サイズを大きくすると共に、空き容量と格納サイズの関係が一定とならないように乱数を用いて調整を加えるというものである。例えば、RAM14の空き容量の所定割合を格納サイズの基準値と決定し、乱数発生部114で発生させた正規分布の乱数によってその基準値に調整を加えることで格納サイズを求める、などの処理となる。格納サイズの決定に際しRAM14の空き容量を考慮することで、格納処理の際のワークメモリ不足を回避することができる。また、乱数により格納サイズを変化させることで、分散格納の規則を分かりにくくすることができ、セキュリティの向上が見込める。

#### 【0039】

RAM14への格納サイズの計算が終わると、格納・消去制御部110は、暗号化されたジョブデータ（以下、混乱のおそれがない場合には単に「ジョブデータ」と呼ぶ）の先頭からその格納サイズ分のデータをRAM14に格納する（S14）。このときのRAM14におけるデータの格納位置（先頭アドレス）は、ランダムに決定しても良いし、所定のルール（空き容量の先頭に格納するなど）に従って決定しても良い。

#### 【0040】

RAM14への格納の後、格納・消去制御部110は、HDD16への格納サイズを計算する（S16）。この格納サイズの計算は、RAM14への格納サイズの計算と同様に行えばよい。

#### 【0041】

HDDへの格納サイズが計算できると、格納・消去制御部110は分散管理情報を作成してHDD16に書き込むと共に（S18）、ジョブデータの未格納部

分の先頭からその格納サイズ分のデータをHDD16に書き込む(S20)。なお、HDD16中には、画像形成装置のオペレーティングシステムにより、当該ジョブデータを格納するためのファイル領域が確保されており、この領域にそれら分散管理情報とジョブデータとを書き込んでいくことになる。

#### 【0042】

以上のステップS12～S20の処理を、ジョブデータの未格納部分がなくなるまで繰り返す(S22)。これにより、ジョブデータがRAM14とHDD16とに分散格納されることになる。このように、図3の処理では、ジョブデータを少量ずつRAM14とHDD16とに交互に格納していく。

#### 【0043】

図3の処理により、HDD16内に生成される格納ファイル40のデータ構造の例を図4に示す。この図に示すように、格納ファイル40は、分散管理情報410と格納ファイルの部分データ450の繰り返しにより構成される。分散管理情報410は、RAM14に格納したデータへのアクセスのための情報であり、部分データ450は、ジョブデータの一部である。この部分データ450は、例えばASN.1のBERエンコーディング規則に従ったデータ構造で記述される。この場合、部分データ450は、当該データの型を示すオブジェクト型452の情報と、そのデータのサイズ454と、そのデータの値456がこの順に並んだものとなる。図3のステップS12からS20の処理を1回行うごとに、分散管理情報410とその次の部分データ450ができる。

#### 【0044】

分散管理情報410のデータ構造の一例を図5に示す。この例では、分散管理情報410は、まずこの管理情報自体の識別子412から始まり、その次にその管理情報自体のサイズ414が記述され、更にその次に、ジョブデータの分散先のデバイス(本実施形態ではRAM14)に格納したデータへのアクセスのための情報420が記述される。情報420は、分散先デバイスの識別子422と、その分散先デバイスに振り分けて記憶したデータのそのデバイス内での記憶位置424と、そのデータのデータサイズ426とを含んでいる。分散先のデバイスがRAM14の場合、記憶位置424としては、例えばRAM14における当該



データの記憶領域の先頭アドレスを用いることができる。

#### 【 0 0 4 5 】

図 1 の例では、ジョブデータを HDD 1 6 と RAM 1 4 とに分散させた。しかし、画像形成装置が HDD 1 6 と RAM 1 4 以外にも記憶装置を備えている場合がある。例えば、画像形成装置が HDD を複数備えていたり、EEPROM や不揮発性 RAM を備えていたりする場合もある。このような場合、ジョブデータをそれら複数の記憶装置に分散格納することもできる。分散先デバイスの識別子 4 2 2 は、それら複数の記憶装置を識別するためのものである。そして、ジョブデータを HDD 1 6 以外に複数の記憶装置に分散格納した場合は、分散管理情報 4 1 0 には、それら各記憶装置ごとに情報 4 2 0 が記述されることになる。この場合、分散管理情報 4 1 0 における情報 4 2 0 の順序が、分散格納したジョブデータの順序に対応する。

#### 【 0 0 4 6 】

次に図 6 を参照して、分散格納したジョブデータを読み出す際の格納・消去制御部 1 1 0 の処理を説明する。

#### 【 0 0 4 7 】

格納・消去制御部 1 1 0 は、ジョブ制御部 1 0 0 からジョブデータファイルの読み出しを要求された場合、まず HDD 1 6 内の当該ファイルの先頭にアクセスし ( S 3 0 ) 、分散管理情報 4 1 0 を読み出し、その分散管理情報 4 1 0 に示される記憶装置識別子 4 2 2 、記憶位置 4 2 4 及びデータサイズ 4 2 6 の情報に従って RAM 1 4 に分散格納したデータを読み出す ( S 3 2 ) 。なお、分散格納先の記憶装置が複数存在する場合には、分散管理情報 4 1 0 中の情報 4 2 0 の順に、それら各記憶装置からデータを読み出して併合していく。このようにしてすべての分散格納先の記憶装置からのデータ読み出しが終わると、その分散管理情報 4 1 0 の直後に格納された部分データ 4 5 0 を読み出し、これを分散先から読み出したデータの後ろに併合する ( S 3 4 ) 。このような処理を、格納ファイル 4 0 の末尾に達するまで繰り返す ( S 3 6 ) ことにより、ジョブデータの読み出しが完了する。なお、読み出したジョブデータは暗号化されているので、格納・消去制御部 1 1 0 はこれを暗号処理部 1 1 2 に復号させてから、ジョブ制御部 1 0

0 に提供する。

【0048】

次に図7を参照して、HDD16とRAM14に分散格納したジョブデータファイルの消去処理を説明する。

【0049】

この消去処理は、ジョブデータファイルに関して所定の消去条件が満たされた時に実行される。代表的な消去条件としては、当該ジョブデータファイルを用いるジョブの実行が完了したことを挙げることができる。またジョブデータファイルを用いるジョブの中止指示がユーザより入力されることも消去条件の一例である。また、ユーザがジョブデータファイルを指定し、そのファイルの消去を明示的に指示することも、消去条件の一例である。

【0050】

格納・消去制御部110は、ジョブ制御部100からのジョブ実行完了通知や、操作パネル12からのユーザの入力を監視し、それら消去条件のいずれかが満たされるのを待つ（S40，S42，S44）。そして、いずれかの消去条件が満足された場合、その条件を満足したジョブのジョブデータファイルのうちのRAM14に格納された部分42を消去する（S46）。消去部分の特定は、例えば格納ファイル中の分散管理情報410を読み出すことで行うことができる。RAM14上のデータなので、高速かつ完全に消去することができる。次に、HDD16内の当該ジョブデータの格納ファイル40を削除して、その格納ファイルの領域を解放する（S48）。この削除処理は、MS-DOS（商標）のDELコマンドや、UNIX（登録商標）のrmコマンドによるファイル削除のように、ファイルシステム上でそのファイルの管理情報を削除する処理でよい。この場合、HDD16には、削除後にも（上書きされるまでは）格納ファイル40の実体データが残ることになるが、残った実体データだけでは元のジョブデータファイルを完全には復元できない。また、本実施形態では、ジョブデータファイルを暗号化してからHDDとRAMに分散格納しているので、HDDに残った実体データだけでは復号が非常に困難になる。

【0051】

格納ファイルの削除（S48）が完了すると、格納・消去制御部110は、ジョブ制御部100に対し、要求されたデータ消去処理が完了した旨を通知する（S50）。この通知を受けたジョブ制御部100は、次のジョブの実行を許可する。これにより、例えば消去の時点で待機中のジョブ（新たなジョブや、別のジョブに割り込まれたジョブなど）があれば、そのジョブの実行が開始又は再開される。

#### 【0052】

このように、本実施形態によれば、RAM14に分散格納したデータを消去することで、HDD16に保存したジョブデータを無効に近い状態とすることができるので、HDDに保存したジョブデータ全体にランダムデータを何度も上書きしていた従来技術と比べて、はるかに高速にデータ消去を行うことが可能となる。このため、割込ジョブからの復帰時や後続のジョブが待機しているような場合でも、待機中のジョブをほとんど待たせることなく、データ消去を行うことができる。したがって、ジョブデータの消去を次のジョブの完了まで先送りにする必要が無くなる。

#### 【0053】

また、本実施形態では、ジョブデータの分散格納先として、揮発性メモリであるRAM14を用いているので、画像形成装置の電源をオフすれば、分散格納したデータも消えてしまうので、上述の消去処理と同様の効果が得られる。

#### 【0054】

なお、1つの例として、上述したRAM14内のデータ消去のあと、適切なタイミングでHDD16上に残った格納ファイルの実体データに対し、ランダムデータの繰り返し上書きによるデータ消去を行うことも好適である。このランダムデータ上書きによる消去処理は、例えば画像形成装置の未使用状態が所定時間続いた時や、節電モードに移行する直前、電源スイッチがオフされた時など、ジョブに影響の少ないときに行うことが好適である。本実施形態では、ジョブ終了後からランダムデータ上書きによるデータ消去を行うまでの間、上記各特許文献に示した従来技術よりもジョブデータを安全に保つことができる。

#### 【0055】

以上に説明した実施形態では、RAM14に分散格納するデータのサイズをRAMの空き容量と乱数に従って決めていたが、これはあくまで一例である。この代わりに、RAM14への格納サイズを固定値としても良いし、空き容量を考慮せずに完全にランダムに決定しても良い。

#### 【0056】

また、RAM空き容量の他の状況も考慮して格納サイズを決めることも好適である。この例を図8に示す。この例では、RAM空き容量(S60)の他に、待機中のジョブの有無(S62)や、画像形成装置全体の処理負荷(S64)、ジョブデータの機密度(S66)、などの情報を取得し、これらの情報をパラメータとしてRAM14への格納サイズを決める(S68)。この計算の基本的な考え方は以下の通りである。

#### 【0057】

まず、待機中のジョブがある場合や、画像処理装置の処理負荷が高い場合は、HDD16へのランダムデータ上書きによるデータ消去がそれだけ遅くなるため、その消去までの時間のジョブデータの安全性を高めるために、RAM14への振り分け量を多くする。これにより、ジョブ完了後のRAM内データ消去によって、より多くのデータが消滅することになるので、ジョブデータの復元の可能性をより減らすことができる。

#### 【0058】

なお、待機中のジョブの有無の情報はジョブ制御部100から、画像処理装置全体の処理負荷はジョブ制御装置100やオペレーティングシステムから、それぞれ取得することができる。

#### 【0059】

また、ジョブデータの機密度が高い場合は、そのデータが不要になった時点で、そのデータのうちできるだけ多くの部分を消すことがセキュリティ上有効である。したがって、機密度が高いほどRAM14へのデータの振り分け量を多くする。

#### 【0060】

ジョブデータの機密度は、ジョブの属性の一つとしてユーザに指定させても良

いし、ジョブの内容から判定しても良い。後者の例としては、例えば親展プリントなど秘密を前提としたジョブの場合は、ジョブデータの機密度を高くするなどである。予めジョブの種類ごとの機密度を画像形成装置に登録しておけばよい。

#### 【0061】

また、HDD16の他にジョブデータを振り分ける記憶装置が複数ある場合、それら複数の記憶装置への振り分け量をそれら記憶装置への書き込み・読み出し速度に応じて決めることも好適である。各記憶装置への書き込み・読み出し速度は、ジョブデータ全体の格納・読み出しの速度に影響するので、書き込み・読み出しが遅い記憶装置へのデータの振り分け量は相対的に小さくすることが好適である。例えば、RAM14の他に、EEPROMにデータを振り分ける場合、EEPROMの書き込み・読み出し速度は、RAM14は当然のこと、HDD16と比べても遅いので、EEPROMへの振り分け量をRAMへの振り分け量よりも小さいものとする。

#### 【0062】

また、ジョブデータの内容に応じた振り分け制御も考えられる。例えば、ジョブデータがヘッダ部とデータ部（ボディ部）から構成される形式であり、ヘッダ部にデータの特徴が多く含まれている場合には、ヘッダ部のデータはRAM14に多く振り分け、ボディ部のデータはHDD16に多く振り分ける、等といった制御などが考えられる。

#### 【0063】

また、以上では、ジョブデータを暗号処理部112で暗号化してから分散格納したが、このような暗号化を行わない場合でも、本発明の分散格納方式はある程度の有効性を持つ。暗号化しなくても、RAM14内のデータ消去により、ジョブデータの一部は消滅するので、万が一HDD16が取り外されるようなことがあっても、完全なジョブデータが漏れることはない。

#### 【0064】

なお、画像形成装置でジョブデータの暗号化を行わない場合、ジョブデータ自体が暗号化されている場合（例えばホストからの印刷データ自体が暗号化されている場合）と、そうでない場合とで、RAM14とHDD16の間のデータ振り

分け割合を変えることも好適である。すなわち、ジョブデータが暗号化されている場合は、RAM内のデータ消去でジョブデータのうちのできるだけ多くの情報が消えるよう、RAMへのデータ振り分け割合を高くするなどである。

#### 【0065】

また、ジョブデータを暗号化せずに分散格納する場合のRAM、HDD間でのデータの振り分け方法として、ジョブデータがタグ付けされた構造化文書の場合、タグ情報（開始タグ、終了タグのうち的一方でも良いし両方でも良い）をRAMに優先的に振り分ける方法が考えられる。この方法では、RAM内のデータ消去により文書構造の情報を消滅させることができる。また、ジョブデータがビジネス文書の場合は文書内の数字情報をRAMに優先的に振り分け、名簿データの場合は人名漢字に該当する文字をRAMに優先的に振り分ける、などと、ジョブデータの種類に応じた特徴部分をRAMに振り分ける方式も好適である。文書の種類は、ジョブデータファイルの属性情報などから求めることができる。

#### 【0066】

また、以上の例では、RAM14とHDD16に交互にジョブデータを振り分けたが、この代わりにそれら両者間での振り分け順序をランダムに変えることも可能である。この場合、分散管理情報410には、各分散格納先に記憶したデータの順序の情報を含める。

#### 【0067】

また以上の例では、分散管理情報410をHDD16に格納したが、これは必須ではない。分散管理情報410のような、各記憶装置へのジョブデータの分散状況を記述した管理情報は、RAM14やその他画像形成装置内の記憶装置に記憶するようにしてもよい。

#### 【0068】

また本実施形態の変形例として、RAM14を利用しない装置構成も考えられる。この例を図9に示す。図9において、図2に示した構成要素と同一又は類似の構成要素には、同一符号を付して説明を省略する。

#### 【0069】

この例では、格納・消去制御部110aは、ジョブデータを暗号処理部112

で暗号化した後、従来と同様HDD16のみに格納する。

#### 【0070】

この変形の特徴は、ジョブデータの消去処理にある。すなわち、図10に示すように、ジョブデータの消去条件が満足された場合（S40～S44）、格納・消去制御部110aは、乱数発生部114に発生させた乱数を用い、HDD16内のジョブデータのうちの消去箇所を決定する（S52）。ここでは、発生させた1乃至複数の乱数を用い、複数の消去箇所について、その位置や消去するデータサイズを決定する。そして、格納・消去制御部110aは、それら決定した消去箇所に対して、ランダムなデータを所定数回繰り返し上書きする（S54）。この上書き消去が完了すると、格納・消去制御部110aは、当該ジョブデータのファイルをファイルシステム上から削除し、ジョブ制御部100に対してデータ消去完了の旨を通知する（S50）。これにより次のジョブが実行可能な状態となり、待機中のジョブや割込などによる中断中のジョブがあれば、それを実行することができる。また、この消去の後、HDD16内に残ったジョブデータの部分に対し、画像形成装置のアイドル時間などに、ランダムデータの繰り返し上書きによる消去処理を施せば、更にセキュリティを向上させることができる。

#### 【0071】

本実施形態によれば、HDD16に格納したジョブデータのうちの複数の消去箇所を消去した時点で、HDD16内に残ったジョブデータは完全なものではなく、仮にその残りデータが取り出されても秘密漏洩のリスクは少なくなる。

#### 【0072】

この例では、暗号化したジョブデータの複数の部分を消去するので、残ったデータを復号するのは非常に困難となる。

#### 【0073】

また、それら消去箇所のサイズのジョブデータ全体に対する比率を小さくしておけば、この消去処理に要する時間は短くて済むため、待機中のジョブをさほど待たせることなく消去処理を実行できる。

#### 【0074】

以上、本発明をデジタル複合機等の画像形成装置に適用した場合の実施形態を

説明した。しかしながら、上述の説明から明らかなように、本実施形態における格納データの秘密保護方式は、処理の種類や格納対象のデータの種類の依存しないので、画像形成装置以外の様々なジョブ処理装置に適用可能である。

【図面の簡単な説明】

【図 1】 実施形態の画像形成装置のハードウェア構成の要部を示す図である。

【図 2】 実施形態の画像形成装置におけるジョブデータファイルの記憶・読み出し・消去のための機構を示す機能ブロック図である。

【図 3】 格納・消去制御部によるジョブデータファイルの格納処理手順の一例を示すフローチャートである。

【図 4】 HDD 内の格納ファイルのデータ構造の例を示す図である。

【図 5】 格納ファイル内の分散管理情報のデータ構造の例を示す図である。

【図 6】 分散格納したジョブデータファイルの読み出し手順の一例を示すフローチャートである。

【図 7】 ジョブデータファイルの消去処理手順の一例を示すフローチャートである。

【図 8】 RAM への格納データ量の決定手順の例を示すフローチャートである。

【図 9】 ジョブデータの格納・消去のための装置の変形例を示す図である。

【図 10】 変形例におけるジョブデータファイルの消去処理手順の一例を示すフローチャートである。

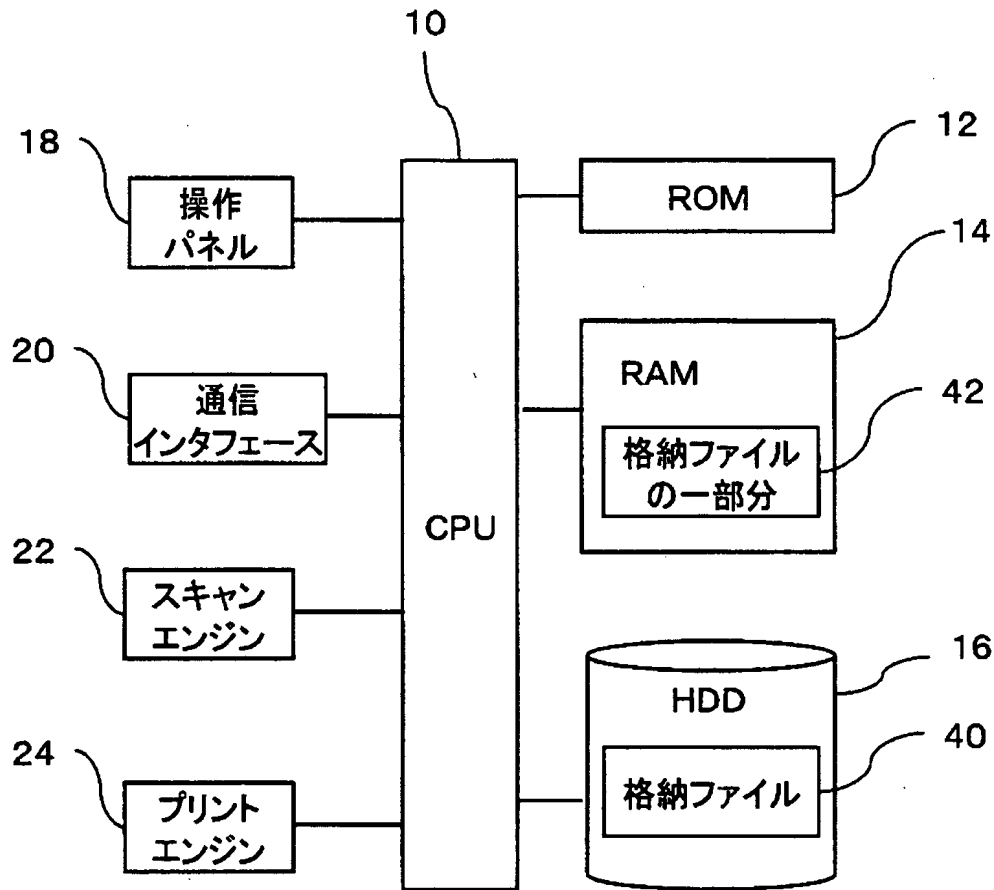
【符号の説明】

10 CPU、12 ROM、14 RAM、16 HDD（ハードディスク・ドライブ）、18 操作パネル、20 通信インタフェース、22 スキャンエンジン、24 プリントエンジン、40 格納ファイル、42 格納ファイルの一部分。

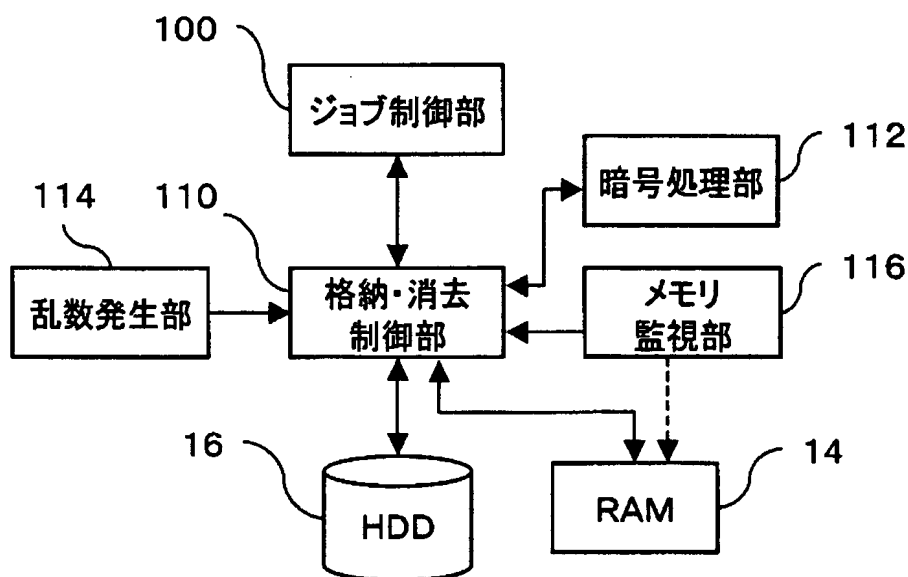


【書類名】 図面

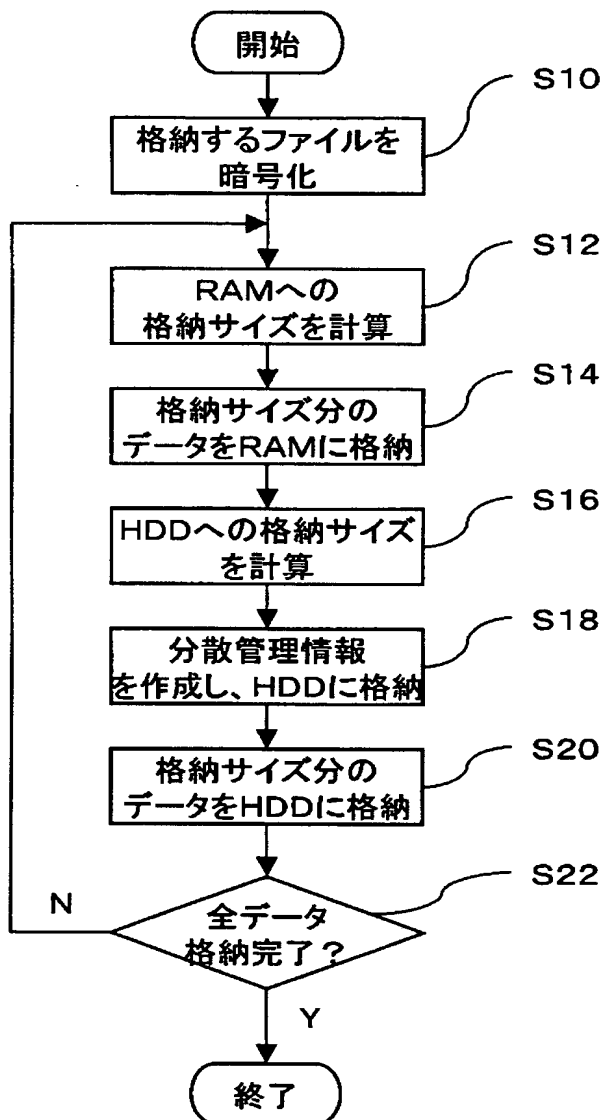
【図1】



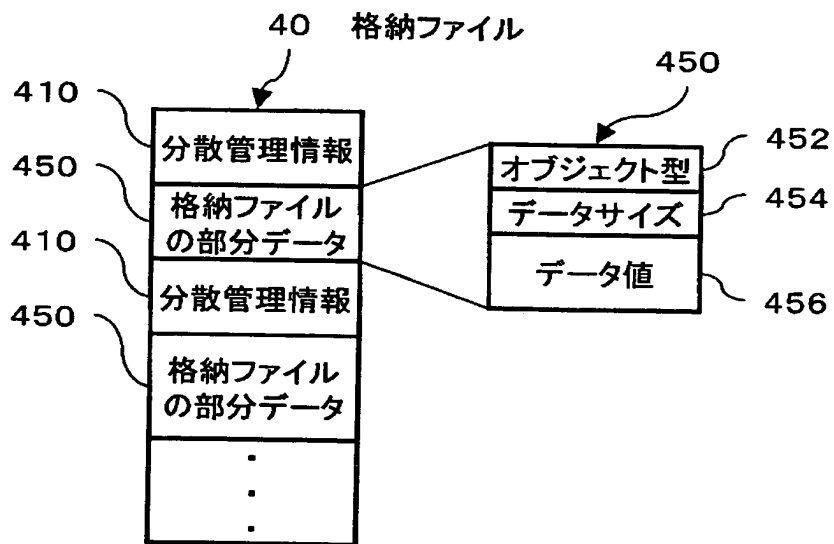
【図2】



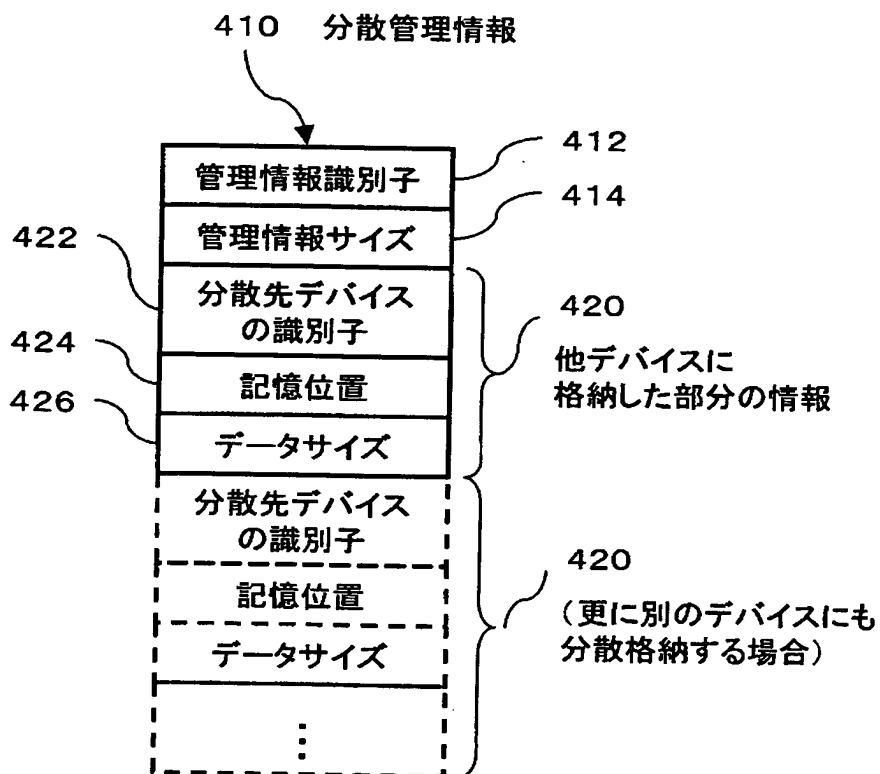
【図 3】



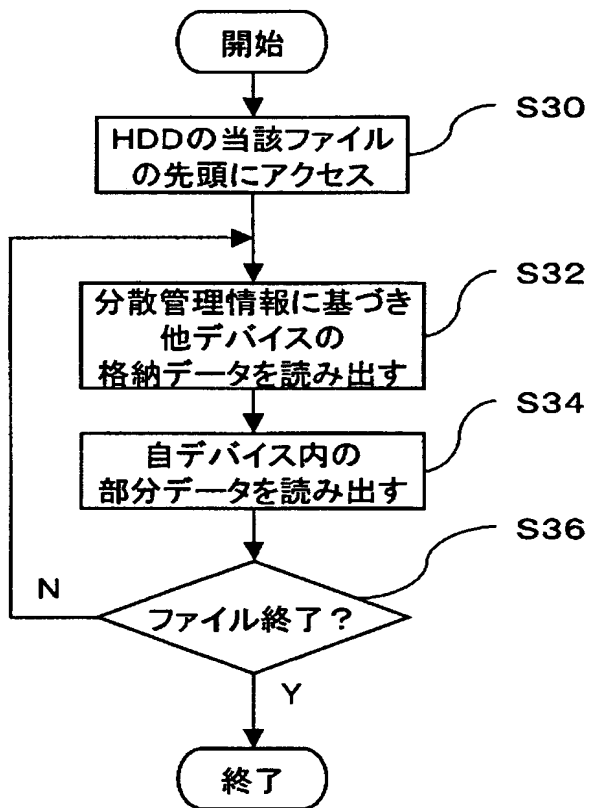
【図 4】



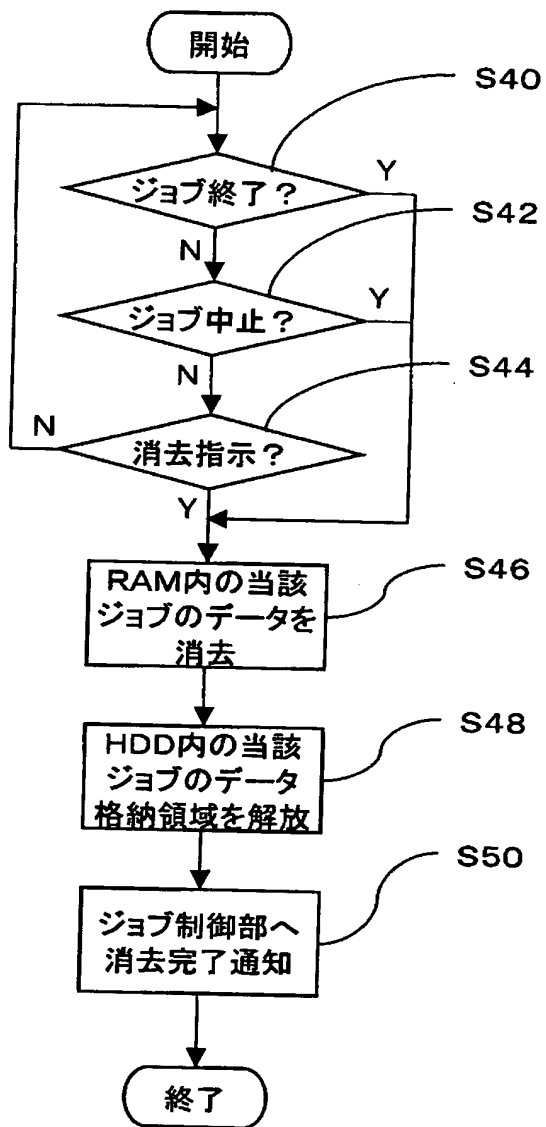
【図 5】



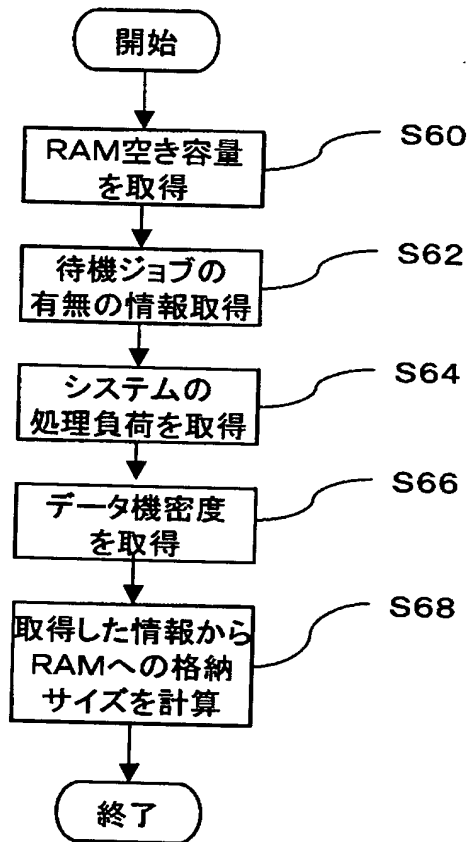
【図 6】



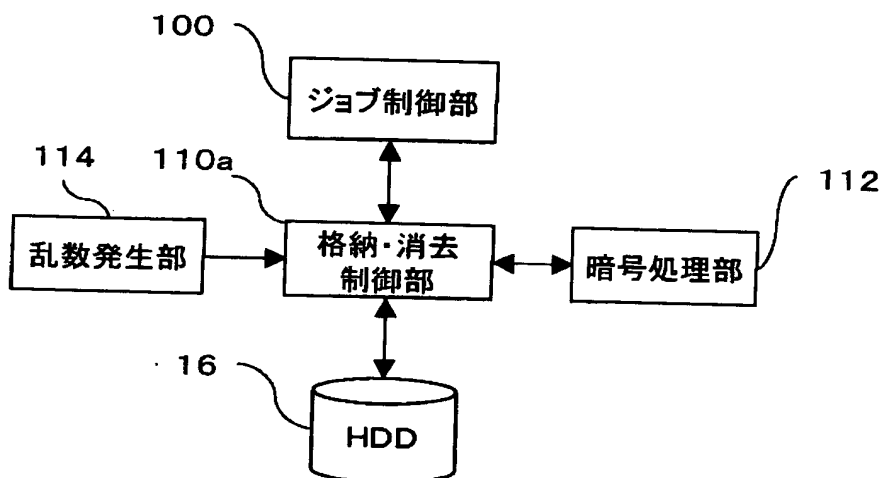
【図 7】



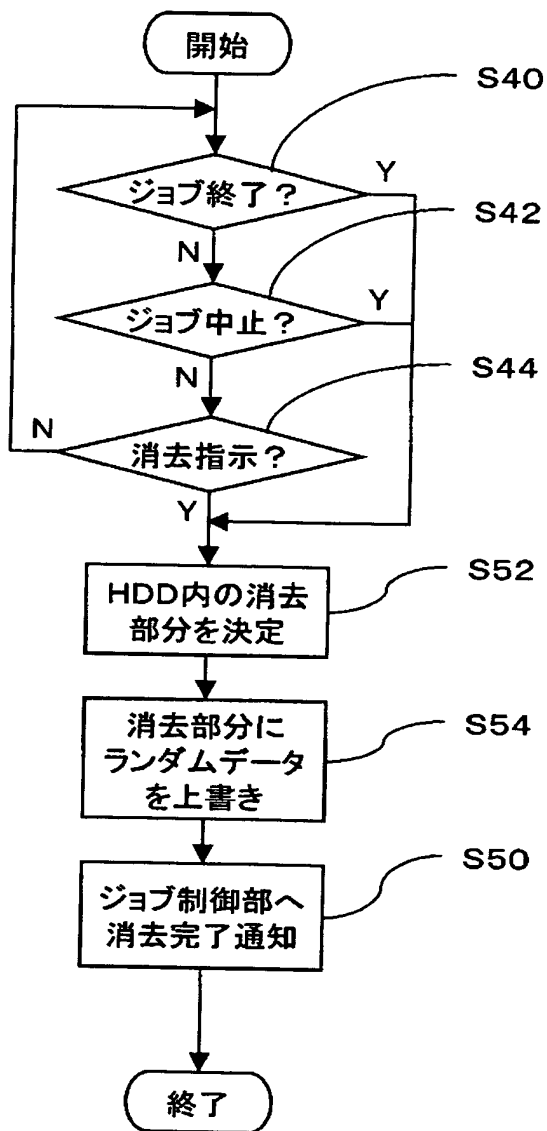
【図 8】



【図 9】



【図 10】



【書類名】 要約書

【要約】

【課題】 画像形成装置等のジョブ処理装置内の大容量記憶装置に格納されるジョブデータのセキュリティを高める。

【解決手段】 CPU 1 0 は、ジョブの実行に必要なジョブデータを保存する際には、そのジョブデータに暗号化を施した上で、その一部分 4 2 を RAM 1 4 に格納し、残りの格納ファイル 4 0 を HDD 1 6 に格納する。ジョブが終了したときには、RAM 1 4 内の当該ジョブのジョブデータの一部分 4 2 を消去する。この消去によりジョブデータ 4 2 の一部分は完全に消滅するので、仮に HDD 1 6 を抜き出して調査されても、完全なジョブデータを知られることはない。

【選択図】 図 1



特願 2 0 0 3 - 0 8 1 4 4 5

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 5 4 9 6 ]

1. 変更年月日

1 9 9 6 年 5 月 2 9 日

[変更理由]

住所変更

住 所

東京都港区赤坂二丁目 1 7 番 2 2 号

氏 名

富士ゼロックス株式会社